AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. – 40. (Canceled)

41. Currently Amended) A computer readable medium comprising a set of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the method of:

in an operating system environment controlled by a single operating system kernel instance,

establishing a global zone [[and]] comprising ~~at least~~ a first non-global zone, wherein the first non-global zone comprises a first file system and wherein the global zone comprises a second file system ~~for isolating processes in the first non-global zone from processes in other non-global zones~~;

receiving, from a first process ~~executing in association with the first non-global zone~~, a first request to perform a first operation, wherein the first process is associated with a first set of privileges and is executed by at least one of the one or more processors, and wherein the first set of privileges restrict the first process to the first non-global zone;

in response to the first request, determining whether performing the first operation is within the first set of privileges ~~enables the first process to obtain additional privileges for which the first process is not authorized~~; and

denying the first request if performing the first operation is not within the first set of privileges ~~enables the first process to obtain additional privileges for which the first process is not authorized~~.

42. – 46. (Cancelled)

47. (Previously Presented) The computer readable medium of claim 41, wherein performing the first operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

48. (Previously Presented) The computer readable medium of claim 41, wherein the first operation includes one of:

mounting/unmounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

49. (Cancelled)

50. (Currently Amended) The computer readable medium of claim 41, wherein the method further comprises:

receiving, from a second process associated with a second set of privileges ~~executing in association with the global zone~~, a second request to perform a second operation, wherein the second process is executing in the global zone, and wherein the second process is executed by at least one of the one or more processors;

in response to the second request, determining whether performing the second operation is within the second set of privileges ~~enables the second process to obtain additional privileges for which the second process is not authorized~~; and

denying the second request if performing the second operation is not within the second set of privileges ~~enables the second process to obtain additional privileges for which the second process is not authorized~~.

51. (Cancelled)

52. (Cancelled)

53. (Previously Presented) The computer readable medium of claim 50, wherein the second operation includes one of:

modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.

54. (New) A system, comprising:

at least one processor; and

a computer readable medium, comprising a set of instructions which, when executed by the at least one processor, cause the at least one processor to perform the method of:

in an operating system environment controlled by a single operating system kernel instance, establishing a global zone comprising a first non-global zone, wherein the first non-global zone comprises a first file system and wherein the global zone comprises a second file system;

receiving, from a first process, a first request to perform a first operation, wherein the first process is associated with a first set of privileges and is executed by at least one of the one or more processors, and wherein the first set of privileges restrict the first process to the first non-global zone;

in response to the first request, determining whether performing the first operation is within the first set of privileges; and

denying the first request if performing the first operation is not within the first set of privileges.

55. (New) The system of claim 54, wherein performing the first operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

56. (New) The system of claim 54, wherein the first operation includes one of:

mounting/unmounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user

57. (New) The system of claim 54, wherein the method further comprises:

receiving, from a second process associated with a second set of privileges, a second request to perform a second operation, wherein the second process is executing in the global zone, and wherein the second process is executed by at least one of the one or more processors;

in response to the second request, determining whether performing the second operation is within the second set of privileges; and

denying the second request if performing the second operation is not within the second set of privileges.

58. (New) The system of claim 57, wherein the second operation includes one of:

modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.